REMARKS

Claims 1-36 are pending in the application.

Claims 1-24 and 26-36 are rejected.

Claims 1-24 and 26-36 remain pending in the application.

Applicants respectfully request reconsideration in light of the remarks contained herein.

Claim Rejections - 35 U.S.C. § 103

Claims 1-3, 6-8, 10-12, 14-20, 22-24, 26-30, and 32-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Secure communications Over Insecure Channels," by Ralph C. Merkle, hereinafter *Merkle*, in view of U.S. Patent No. 5,825,890 to Elgamal et al., hereinafter *Elgamal*.

Applicant respectfully submits that *Merkle* and *Elgamal*, alone or in combination, do not disclose each element of Claim 1. For example, the Applicant respectfully submits that neither *Merkle* nor *Elgamal* disclose "adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair; [and] encrypting the token with the added randomization information at the receiver, the token corresponding with the randomly selected encryption-decryption function pair," as required by Claim 1.

The Office Action states:

> 7. As per claims 1, 6, 14, 28, and 33, Merkle teaches creating a set of N trap door encryption-decryption function pairs each paired with a corresponding token; transmitting the set of N trap door encryption-decryption function pairs along with a corresponding token to a receiver', randomly selecting at the receiver one of the trap door encryption-decryption function pairs and the corresponding token; recording in a key escrow database the created set of N trap door encryption decryption function pairs and the corresponding paired token; recording in the key escrow database the randomly selected trap door encryption decryption function pair along with the encrypted token; and inverting the

> created set of N trap door encryption-decryption function pairs and the randomly selected trap door encryption-decryption function pair along with the encrypted token to identify the decryption key (pages 296-299).
>
> 8. Merkle does not disclose adding randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypting the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair.
>
> 9. Elgamal teaches adding padding information to data prior to encrypting the data (column 17, lines 21-40).
>
> 10. It would have been obvious to one of ordinary skill in the ad at the time the invention was made to add randomization information at the receiver to the corresponding token of the selected trap door encryption-decryption function pair and encrypt the token with the added randomization information, the token corresponding with the randomly selected encryption-decryption function pair, as apposed to sending it back unencrypted as Merkle suggests, since Elgamal discloses at column 17, lines 21-40 that such a modification would allow secure distribution of information by making the intended data the appropriate length for block ciphers, as well as provide a method for the receiver to detect whether the data has been tampered with.

Office Action, at 2-3

First, Applicant respectfully disagrees that the cited portion of *Elgamal* supplies the above-identified missing elements. The cited portions of *Elgamal* discusses "padding data [that] is used to make the record length be a multiple of the block ciphers block size when a block cipher is used for encryption." *Elgamal*, 17:22-25. *Elgamal*'s "padding data" is not randomization data, as required by the claim. This is exemplified by *Elgamal* saying that "[t]he actual value of the padding data is unimportant." *Elgamal*, 17:29-31. Therefore, *Elgamal* does not disclose, teach, or suggest "adding randomization information," as required by the claim. Moreover, claim 1 requires that the randomization information be added at the receiver and that the receiver encrypt the token with the added randomization information. The cited portion of *Elgamal*, however, does not disclose which party adds the padding data.

Furthermore, the Office Action's rationale for the combination of *Merkle* and *Elgamal* similarly fails to compensate for the deficiencies in the references. The Examiner cited *Elgamal*, 17:21-40 to show that it would have been obvious to add the missing claim elements. As

Applicant has already shown, the cited portion of *Elgamal* does not show adding randomization information, as required by the claim.

Second, even assuming for purposes of argument that the proposed combination discloses the limitations of Applicant's claims, which Applicant disputes, it would not have been obvious to one skilled in the art to make the combination. The cited portion of *Elgamal* does not mention "allow[ing] secure distribution of information . . . [or] provid[ing] a method for the receiver to detect whether the data has been tampered with." Office Action, at 3. Without citation to evidence from the references, this motivation for combination appears to be based on Applicant's own disclosure, which is improper.

For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claim 1.

The Examiner also relies on the *Merkle-Elgamal* combination to reject independent Claims 6, 14, 28, and 33. Applicant respectfully submits that the proposed *Merkle-Elgamal* combination does not disclose, teach, or suggest each and every element of Applicant's independent claims. Thus, for reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Elgamal* disclose, teach, or suggest each and every element as set forth in Applicant's independent Claims 6, 14, 28, and 33.

Dependent Claims 2 and 3 depend from independent Claim 1, dependent Claims 7, 8, and 10-12 depend from independent Claim 6, dependent Claims 29-30 and 32 depend from independent Claim 28, and dependent claims 34-36 depend from independent Claim 33. Applicant has shown each of the independent claims to be allowable. Accordingly, dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36 are not obvious over the *Merkle-Elgamal* combination at least because they include the limitations of their respective independent claims.

Additionally, dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36 recite elements that further distinguish the art. Claim 3 recites "randomly selecting at the receiver an additional trap door encryption-decryption function pair and the corresponding token" and "adding randomization information to the corresponding token of the additional selected trap door encryption-decryption function pair." Claims 7, 20, 22, 30, 34, and 36 recite certain similar, though not identical, features and operations. The Office Action states:

> 12. As per claims 3, 7, 14, 30 and 36, Merkle does not explicitly teach the receiver selecting more than one of the puzzles to decrypt. Clearly from the teachings of Merkle one of ordinary skill in the art would know that the work needed to be performed by an eavesdropper plotting to learn the decryption key is $O(n)^2$. Having the receiver choose more than one puzzles slightly increases the poor security of Merkle's system by forcing the eavesdropper to perform more calculations.

Office Action, page 4.

Applicant disagrees. The Office Action does not cite any portion of *Merkle, Elgamal*, or any other evidence to support this conclusion. Therefore, the rejection of claims 3, 7, 20, 22, 30, 34, and 36 is improper. For reasons similar to those discussed above with regard to Claim 1, Applicant respectfully submits that neither *Merkle* nor *Elgamal* disclose, teach, or suggest the features and operations recited in dependent Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 2, 3, 7, 8, 10-12, 29-30, 32, and 34-36.

Claims 4, 5, 9, 13, 21, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Merkle*, in view of *Elgamal.*, and further in view of U.S. Patent No. 5,815,573 to Johnson, *et al.,* hereinafter *Johnson*. Dependent claims 4 and 5 depend from independent Claim 1, dependent claims 9, 13, and 21 depend from independent Claim 6, and dependent claim 31 depends from independent Claim 28. Applicant has shown that each of the independent Claims are allowable. For at least this reason, Applicant respectfully requests reconsideration and allowance of Claims 4, 5, 9, 13, 21, and 31.

Additionally, the Examiner has not made a *prima facie* showing of obviousness with respect to each of these claims. For example, with respect to claims 4, 5, and 31 the Examiner asserts that the combination of *Merkle, Elgamal*, and *Johnson* is motivated because "it would associate a key to a user with provable certainty." Office Action, at 7. The Office Action does not cite any discussion in *Merkle, Elgamal*, *Johnson*, or any other evidence to support this contention. Similarly, the Office Action does not cite any portion of *Merkle, Elgamal*, or *Johnson* to support the motivation contentions with respect to claims 9, 13, and 21. For at least these reasons, Applicant respectfully requests reconsideration and allowance of Claims 4, 5, 9, 13, 21, and 31.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clear and apparent, Applicant respectfully requests reconsideration and allowance of the pending claims.

Applicant believes no fees are due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

If there are matters that can be discussed by telephone to advance prosecution of this application, Applicant invites the Examiner to contact its attorney at the number provided below.

Respectfully submitted,

Baker Botts L.L.P.
Attorneys for Applicant

/Bradley S. Bowling/_____
Bradley S. Bowling
Reg. No. 52,641

Dated: June 6, 2006

CORRESPONDENCE ADDRESS:

Customer No. 05073